(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002351743 A**

(43) Date of publication of application: **06.12.02**

(51) Int. Cl **G06F 12/14**
G06F 3/12
H04L 9/08

(21) Application number: **2001155832**

(22) Date of filing: **24.05.01**

(71) Applicant: **FUJI XEROX CO LTD**

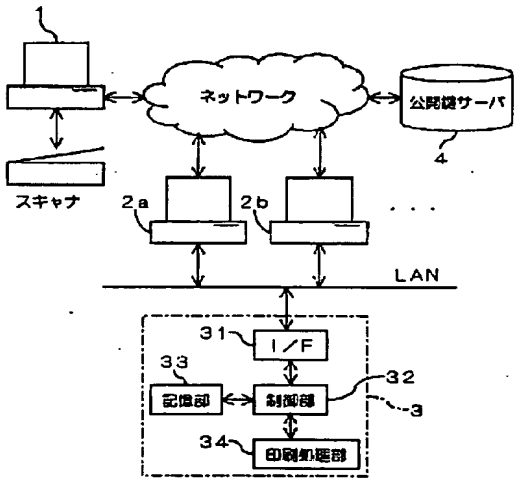
(72) Inventor: **SATO TAKANE**

(54) DOCUMENT DISTRIBUTION SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a document distribution system which can improve security.

SOLUTION: A transmission-side computer 1 generates a document only for browsing according to an original document, specifies a printer 3 which is made to print the original document, obtains a ciphering key related to the printer 3 from an open key server 4, and generates a ciphered document by ciphering the original document with the obtained ciphering key. Then a document container containing the document only for browsing and the ciphered document is distributed to a reception-side computer 2, which displays the document only for browsing and outputs the ciphered document to the printer 3 as instructed. The printer 3 deciphers the ciphered document by using a deciphering key stored in a storage part 33 and prints the document.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－351743
（P2002－351743A）
(43)公開日　平成14年12月6日(2002.12.6)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ	５Ｂ０１７
			３２０Ｂ	５Ｂ０２１
3/12		3/12	Ａ	５Ｊ１０４
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	

審査請求　未請求　請求項の数９　ＯＬ　（全７頁）

(21)出願番号　特願2001－155832(P2001－155832)

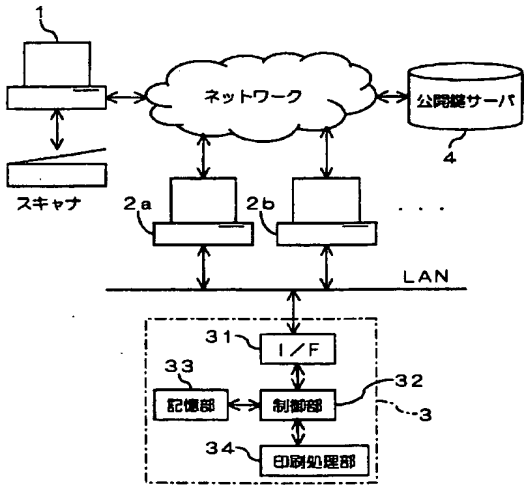
(22)出願日　平成13年５月24日(2001.5.24)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　佐藤　高根
神奈川県川崎市高津区坂戸３丁目２番１号
ＫＳＰ　Ｒ&Ｄ　ビジネスパークビル
富士ゼロックス株式会社内
(74)代理人　100075258
弁理士　吉田　研二　（外２名）

Ｆターム(参考)　5B017 AA03 AA06 BA07 BA09 CA16
5B021 AA01 BB04 BB09 CC05 EE03
5J104 AA01 AA32 NA02 PA14

(54)【発明の名称】　文書配信システム

(57)【要約】
【課題】　セキュリティを向上できるできる文書配信システムを提供する。
【解決手段】　送信側コンピュータ１がオリジナル文書に基づいて閲覧専用文書を生成するとともに、そのオリジナル文書を印刷させるプリンタ３を特定し、そのプリンタ３に関連する暗号鍵を公開鍵サーバ４から取得して、当該取得した暗号鍵でオリジナル文書を暗号化した暗号化文書を生成する。そして、閲覧専用文書と暗号化文書とを含めた文書コンテナを受信側コンピュータ２に配信し、受信側コンピュータ２が閲覧専用文書を表示するとともに、指示により暗号化文書をプリンタ３に出力し、プリンタ３が記憶部３３に記憶している復号鍵を用いて暗号化文書を復号化して印刷処理する文書配信システムである。



1

【特許請求の範囲】

【請求項１】　文書の提供元に配置され、オリジナル文書に基づき、所定の印刷装置でのみ復号可能な暗号化処理を行って得られた暗号化文書並びに、閲覧専用文書を生成し、当該生成した暗号化文書並びに、閲覧専用文書を文書コンテナとして配信する文書提供装置と、

前記文書提供装置から配信された文書コンテナを受信し、当該文書コンテナに含まれる閲覧専用文書を閲覧に供するとともに、指示に応じて当該文書コンテナに含まれる暗号化文書を、それを復号可能な印刷装置に出力する文書取得装置と、

前記文書取得装置から入力される暗号化文書を復号化してオリジナル文書を再生し、当該再生したオリジナル文書の印刷を行う印刷装置と、

を有し、

文書提供装置側で選択した暗号化処理により、印刷先の印刷装置を提供元で特定可能としたことを特徴とする文書配信システム。

【請求項２】　請求項１記載の文書配信システムにおいて、さらに、

前記文書提供装置は、文書コンテナに含める暗号化文書に、当該暗号化文書の印刷時にオーバーレイ印刷されるべき情報を含めて配信し、

前記印刷装置は、前記暗号化文書を復号化して得たオリジナル文書を、前記オーバーレイ印刷されるべき情報とともに印刷することを特徴とする文書配信システム。

【請求項３】　印刷対象として暗号化文書の入力を受けて、当該暗号化文書を事前に設定された復号化処理によって復号化する手段と、

前記復号化処理によって得られたオリジナル文書を印刷する手段と、

を一体に備えたことを特徴とする印刷装置。

【請求項４】　請求項３に記載の印刷装置において、

前記暗号化文書に対し、その文書とともにオーバーレイ印刷されるべき付加情報が含まれているときには、当該暗号化文書を復号化して得たオリジナル文書を印刷するとともに、前記付加情報をオーバーレイ印刷することを特徴とする印刷装置。

【請求項５】　出力対象として入力される暗号化文書を事前に設定された復号化処理によって復号化する手段と、

前記復号化処理によって得られたオリジナル文書を所定の態様で出力する手段と、

を一体に備えたことを特徴とする出力装置。

【請求項６】　オリジナル文書を配信するために、その配信先に配置された印刷装置に固有に設定された復号化処理にて復号可能なように、オリジナル文書を暗号化し、暗号化文書を生成する手段と、

当該暗号化文書を配信する手段と、

を有し、オリジナル文書の配信元でそのオリジナル文書の印刷を行わせる印刷装置を特定可能としたことを特徴とする文書配信装置。

2

【請求項７】　オリジナル文書の配信先に配置された印刷装置に固有に設定された復号化処理にて復号可能なように、オリジナル文書を暗号化し、暗号化文書を生成する工程と、

当該暗号化文書を配信する工程と、

を有し、オリジナル文書の配信元でそのオリジナル文書の印刷を行わせる印刷装置を特定可能としたことを特徴とする文書配信方法。

【請求項８】　印刷装置に内蔵されたマイクロコンピュータに、

暗号化文書の入力を受け付ける手順と、

当該暗号化文書を事前に設定された復号化処理にて復号化する手順と、

当該復号化して得られたオリジナル文書を印刷するための制御を行う手順と、

を実行させることを特徴とするプログラム。

【請求項９】　文書の提供元に配置され、配信対象となったオリジナル文書を読み取るとともに、事前に設定された暗号鍵により暗号化処理して暗号化文書を生成して出力するスキャナと、

前記スキャナから入力される暗号化文書を配信する文書提供装置と、

前記文書提供装置から配信された暗号化文書を受信し、当該暗号化文書を前記スキャナを識別する情報に関連づけられた復号鍵で復号し、オリジナル文書を再生する文書取得装置と、を含み、

文書の提供元で行われた暗号化処理により、文書の取得側で文書の入力に用いられたスキャナを特定可能としたことを特徴とする文書配信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、配信される文書の印刷を行うための文書配信システムに係り、特に文書の漏洩点を特定するための改良に関する。

【０００２】

【従来の技術】近年、電子メールやＷｅｂサーバなどを利用した電子的な文書配信技術が発展している。これらの技術では配信対象となっている電子的文書を誰もがアクセスできる反面、セキュリティが低下するとの懸念がある。すなわち、電子メールやＷｅｂサーバの利用者は、その文書の原本（オリジナル文書）を自己の使用するパーソナルコンピュータ上で再生し、このオリジナル文書に対して、表示、印刷などの操作のほか、加工、複写、転送などの処理が可能となる。

【０００３】そこでこれら電子的文書に対して正当な配信先が公開している暗号鍵を用いて暗号化処理を行い、相手側で当該公開鍵に対応して秘密に保持する復号鍵にて復号するシステム（公開暗号鍵方式）がある。これに

よると上記のようなセキュリティ低下の懸念は少なくなる。Ｗｅｂサーバから取得できる文書は暗号化された状態にあるためである。

【０００４】ところが、近年の情報漏洩の態様として配信先の組織内での情報漏洩の問題がある。具体的には一旦暗号化文書として正当に配信を受け、これを復号化した者が、当該復号化後のオリジナル文書をコンピュータ内に保存しておくことによって電子的に漏洩したり、印刷によって紙となったものが複写等を通じて流通してしまうのである。

【０００５】ここで、後者のように紙からの複写に対しては「禁複写」のごとき文字列が複写時に浮かび上がるようにする特殊な印刷技術（いわゆる「桜紙印刷」）が知られている。

【０００６】

【発明が解決しようとする課題】しかしながら、上記従来の桜紙印刷などの技術では、漏洩情報の出所が電子的に保存されたオリジナル文書を不正にコピーしたことによるのか、印刷されたものが複写などによって流通したものかが区別できない。

【０００７】また、従来の公開鍵暗号方式では、公開鍵が配信先の人物に対して発行されるものであるため、当該公開鍵により暗号化されているオリジナル文書の取り扱いは、当該配信先の人物に委ねられている。したがって、配信元の利用者が情報の出所を指定することはできず、出所特定が困難になってセキュリティの向上に資することができないという問題点があった。

【０００８】本発明は上記実情に鑑みて為されたもので、配信元の利用者が情報の出所を特定できるようにして、セキュリティの向上を図ることのできる文書配信システムを提供することを目的とする。

【０００９】

【課題を解決するための手段】上記従来例の問題点を解決するための本発明は、文書配信システムにおいて、文書の提供元に配置され、オリジナル文書に基づき、所定の印刷装置でのみ復号可能な暗号化処理を行って得られた暗号化文書並びに、閲覧専用文書を生成し、当該生成した暗号化文書並びに、閲覧専用文書を文書コンテナとして配信する文書提供装置と、前記文書提供装置から配信された文書コンテナを受信し、当該文書コンテナに含まれる閲覧専用文書を閲覧に供するとともに、指示に応じて当該文書コンテナに含まれる暗号化文書を、それを復号可能な印刷装置に出力する文書取得装置と、前記文書取得装置から入力される暗号化文書を復号化してオリジナル文書を再生し、当該再生したオリジナル文書の印刷を行う印刷装置と、を有し、文書提供装置側で選択した暗号化処理により、印刷先の印刷装置を提供元で特定可能としたことを特徴としている。これにより情報の出力点としての印刷装置を文書の提供元で指定でき、情報流通の出所を容易に特定できるようにしてセキュリティを向上できる。

【００１０】ここで文書提供装置は、文書コンテナに含める暗号化文書に、当該暗号化文書の印刷時にオーバーレイ印刷されるべき情報を含めて配信し、前記印刷装置は、前記暗号化文書を復号化して得たオリジナル文書を、前記オーバーレイ印刷されるべき情報とともに印刷することが好ましい。このオーバーレイ印刷により桜紙の設定を提供元で設定でき、セキュリティの向上に資することができる。

【００１１】上記従来例の問題点を解決するための本発明は、印刷装置において、印刷対象として暗号化文書の入力を受けて、当該暗号化文書を事前に設定された復号化処理によって復号化する手段と、前記復号化処理によって得られたオリジナル文書を印刷する手段と、を一体に備えたことを特徴としている。

【００１２】ここで暗号化文書に対し、その文書とともにオーバーレイ印刷されるべき付加情報が含まれているときには、当該暗号化文書を復号化して得たオリジナル文書を印刷するとともに、前記付加情報をオーバーレイ印刷することも好ましい。

【００１３】さらに上記従来例の問題点を解決するための本発明は、出力装置において、出力対象として入力される暗号化文書を事前に設定された復号化処理によって復号化する手段と、前記復号化処理によって得られたオリジナル文書を所定の態様で出力する手段と、を一体に備えたことを特徴としている。

【００１４】さらに上記従来例の問題点を解決するための本発明は、文書配信装置において、オリジナル文書を配信するために、その配信先に配置された印刷装置に固有に設定された復号化処理にて復号可能なように、オリジナル文書を暗号化し、暗号化文書を生成する手段と、当該暗号化文書を配信する手段と、を有し、オリジナル文書の配信元でそのオリジナル文書の印刷を行わせる印刷装置を特定可能としたことを特徴としている。

【００１５】また、上記従来例の問題点を解決するための本発明は、文書配信方法において、オリジナル文書の配信先に配置された印刷装置に固有に設定された復号化処理にて復号可能なように、オリジナル文書を暗号化し、暗号化文書を生成する工程と、当該暗号化文書を配信する工程と、を有し、オリジナル文書の配信元でそのオリジナル文書の印刷を行わせる印刷装置を特定可能としたことを特徴としている。

【００１６】上記従来例の問題点を解決するための本発明は、印刷装置に内蔵されたマイクロコンピュータに実行させるプログラムであって、暗号化文書の入力を受け付ける手順と、当該暗号化文書を事前に設定された復号化処理にて復号化する手順と、当該復号化して得られたオリジナル文書を印刷するための制御を行う手順と、を行わせることを特徴としている。

【００１７】さらに、上記従来例の問題点を解決するた

めの本発明は、文書配信システムにおいて、文書の提供元に配置され、配信対象となったオリジナル文書を読み取るとともに、事前に設定された暗号鍵により暗号化処理して暗号化文書を生成して出力するスキャナと、前記スキャナから入力される暗号化文書を配信する文書提供装置と、前記文書提供装置から配信された暗号化文書を受信し、当該暗号化文書を前記スキャナを識別する情報に関連づけられた復号鍵で復号し、オリジナル文書を再生する文書取得装置と、を含み、文書の提供元で行われた暗号化処理により、文書の取得側で文書の入力に用いられたスキャナを特定可能としたことを特徴としている。

【００１８】

【発明の実施の形態】［実施形態１］本発明の第１の実施の形態について図面を参照しながら説明する。本発明の第１の実施の形態に係る文書配信システムは、図１に示すように、文書の提供元に置かれた文書提供装置としての送信側コンピュータ１と、文書の提供先に置かれた複数の文書取得装置としての受信側コンピュータ２ａ，２ｂ，…と、印刷装置としてのプリンタ３と、公開鍵サーバ４とから基本的に構成され、送信側コンピュータ１と受信側コンピュータ２と公開鍵サーバ４とは相互に通信可能なようにネットワークを介して接続され、プリンタ３は、受信側コンピュータ２と相互に通信できるようにＬＡＮ（Local Area Network）を介して接続されている。尚、送信側コンピュータ１及び受信側コンピュータ２は、いずれも一般的なパーソナルコンピュータである。尚、ネットワークには文書の提供先とプリンタとがさらに数多く接続されているのが実際の状態であるが、ここでは説明のため、これらの記載を省略している。

【００１９】またプリンタ３は、データインタフェース（Ｉ／Ｆ）３１と、制御部３２と、記憶部３３と、印刷処理部３４とを含んでいる。公開鍵サーバ４は、図２に示すように、プリンタを識別する情報（組織名、装置名、イーサネット（登録商標）アドレス、ＩＰアドレス等）と、プリンタが固有に記憶する復号鍵に対応する暗号鍵とを関連づけたテーブルを記憶している。

【００２０】送信側コンピュータ１は、操作者の指示により、配信の対象となる電子文書の原本（オリジナル文書）を印刷させるプリンタ３に対応する暗号鍵を公開鍵サーバ４から取得する。そして、この暗号鍵を用いてオリジナル文書を暗号化処理する。この暗号化処理は広く知られた公開鍵暗号方式におけるものと同様であるので、その詳細な説明を省略する。また、この送信側コンピュータ１は、当該暗号化処理後のオリジナル文書（暗号化文書）をネットワークを介して配信する。具体的に送信側コンピュータ１は、スキャナによって読み取った画像データをオリジナル文書として処理することとしてもよいし、ワードプロセッサなどによって生成したデータをオリジナル文書として処理してもよい。

【００２１】受信側コンピュータ２では、この暗号化文書の配信をネットワークを介して受けて記憶する。ここで暗号化文書はプリンタ３に固有の復号鍵でのみ復号可能であるので、利用者は受信側コンピュータ２の上でオリジナル文書を得ることはできない。また、この受信側コンピュータ２は、利用者からの指示を受けて、当該暗号化文書をプリンタ３にＬＡＮを介して出力する。

【００２２】プリンタ３は、複数の受信側コンピュータ２ａ，２ｂ，…によって共用されるものである。プリンタ３のデータインタフェース３１は、ＬＡＮに接続され、受信側コンピュータ２のいずれかからＬＡＮを介して入力されるデータを制御部３２に出力する。

【００２３】制御部３２は、データインタフェース３１を介して入力されるデータが暗号化文書でない場合には、当該データに基づいて印刷処理部３４を制御し、印刷を行う。また、当該データが暗号化文書であれば復号化処理を開始する。すなわち、暗号化文書の入力を受けた制御部３２は、記憶部３３に記憶されている復号化処理用のプログラムを起動し、まず記憶部３３から秘密に保持されている復号鍵を読み出す。そして、この復号鍵を用いて暗号化文書を復号化してオリジナル文書を生成する。制御部３２は、このオリジナル文書に基づいて印刷処理部３４を制御し、当該オリジナル文書の内容を印刷する。尚、制御部３２は例えば、入力されたデータに基づいて印刷処理部３４を制御するための処理言語（Ｐｏｓｔｓｃｒｉｐｔ（商標）等の言語）を用いた指示を生成し、この指示を印刷処理部３４に出力することによって印刷処理を実行する。

【００２４】記憶部３３は、制御部３２によって実行されるプログラムを格納している。またこの記憶部３３は、固有に設定された復号鍵を保持している。印刷処理部３４は、制御部３２から入力される指示に従って、印刷を実行する。

【００２５】このように、本実施の形態において特徴的なことは、プリンタ３のような最終出力点をなす装置に復号化の処理が一体的に取り込まれていることである。すなわち出力処理の一環として復号化の処理が行われることで、復号化により得られたデータが他の出力装置へ漏洩することがなく、従って情報の出所が特定されるのである。また、最終出力点である装置を文書の提供元が暗号化処理を利用して特定することにより、簡便な構成で、出所を提供元で指定できるようになっている。

【００２６】また、送信側コンピュータ１は、暗号化文書のみならず、その内容がどのようなものであるかを伝達するために、閲覧専用の文書を生成して、暗号化文書とともに配信を行うことが好ましい。ここでは、暗号化文書と閲覧専用の文書とをセットとしたものを「文書コンテナ」と称する。このようにすると、受信側コンピュータ２において、そのオリジナル文書を生成することなしに、文書の内容がどのようなものかを確認できる。こ

の閲覧専用文書はオリジナル文書を表示した際の画面のハードコピーや当該ハードコピーの一部を隠蔽処理したビットマップ画像データとすることが好ましい。これにより、当該閲覧専用文書からオリジナル文書を容易に再生できない状態を維持しつつ、内容の見読性（確認のしやすさ）を向上できる。

【００２７】次に、本実施の形態に係る文書配信システムの動作について説明する。送信側コンピュータ１が、その利用者の指示に従い、配信対象となる電子文書（オリジナル文書）から閲覧専用文書を生成する。また、配信先で印刷をさせるプリンタ３に対応する暗号鍵をネットワークを介して公開鍵サーバ４から取得し、この暗号鍵を用いてオリジナル文書を暗号化して暗号化文書を生成する。

【００２８】送信側コンピュータ１は、これら閲覧専用文書と暗号化文書とをセットとした文書コンテナを生成し、これをネットワークを介して受信側コンピュータ２に送信する。受信側コンピュータ２では、利用者の指示に応じて、受信した文書コンテナに含まれる閲覧専用文書をディスプレイに表示させて利用者に提示する。また、利用者が印刷を指示したときには、暗号化文書をＬＡＮを介してプリンタ３に出力する。

【００２９】プリンタ３では、入力された暗号化文書に対し、記憶部３３内に事前に設定された復号鍵を用いて復号化処理を行う。そして、復号化処理によって得たオリジナル文書を印刷処理する。

【００３０】一方、送信側コンピュータ１の利用者の意図しない別のプリンタ３′（図示せず）に対し出力指示が行われたときには、プリンタ３′に設定されている復号鍵が異なるため、正しく復号することができず、オリジナル文書の印刷は行われない。また、本実施の形態に係るプリンタ３ではなく、通常のプリンタに出力された場合には、暗号化文書そのものが印刷されるため、意味のない文字列が印字されることとなる。

【００３１】このように、本実施の形態によれば、送信側コンピュータ１の利用者の意思に応じて出力点であるプリンタが選択されるため、出所が明確になりセキュリティの向上に資することができる。

【００３２】尚、このようにして印刷を行う場合にも、桜紙印刷の技術を組み合わせることにより、さらにセキュリティの向上を図ることができる。すなわち、この場合には提供元においてオリジナル文書に重ね合わせて（オーバーレイして）印刷されるべき情報を当該オリジナル文書に設定しておき、当該設定後のオリジナル文書を暗号化する。この場合には、プリンタ３の制御部３２が復号化して得たオリジナル文書を印刷する際に、当該オリジナル文書に含まれているオーバーレイ印刷されるべき情報をオリジナル文書に重ね合わせて印刷する。

【００３３】ここで、オーバーレイ印刷されるべき情報としては、暗号化されていたことを示す文字列や、宛先（受取人）の氏名や名称、あるいは印刷時刻を印字すべき指示などがある。

【００３４】また、ここまでの説明では、オリジナル文書自体を暗号化して暗号化文書を生成していたが、オリジナル文書から印刷処理用の制御言語での記述に変換し、この変換後の記述を暗号化して暗号化文書として送信してもよい。この場合には、プリンタ３の制御部３２は、当該暗号化文書を復号化し、そのまま印刷処理部３４に出力する。そして印刷処理部３４が当該復号された記述に基づいて印刷を実行する。

【００３５】尚、ここまでの説明では、文書コンテナの受け渡しに際し、送信側コンピュータ１が受信側コンピュータ２に対して送信するとして説明したが、具体的にはネットワーク上に文書コンテナを蓄積する文書管理装置を接続し、当該文書管理装置に送信側コンピュータ１が文書コンテナを格納して、その格納場所を特定する情報（ＵＲＬ等）を電子メールなどで受信側コンピュータ２に配信することで受信側コンピュータ２への送信を実行してもよい。この場合には、受信側コンピュータ２は、当該受信したＵＲＬを参照して文書管理装置にアクセスし、指定された文書コンテナを取得する。

【００３６】［実施形態２］さらに、この第１の実施の形態においては文書の提供先を認証するようにしていたが、受信側から送信側を認証するシステムとすることも可能である。すなわち、本発明の第２の実施の形態に係る文書配信システムは、送信側コンピュータ１を認証するために署名情報を用いるもので、その構成は図１に示した第１の実施の形態のものと同様のものであるが、送信側コンピュータ１及びプリンタ３の処理が若干異なり、公開鍵サーバ４が送信側コンピュータ１を識別する情報に関連づけて、当該送信側コンピュータ１から受信された暗号化文書を復号するための復号鍵を保持しており、要求に応じて当該復号鍵を提供する。

【００３７】すなわち、本実施の形態の送信側コンピュータ１は、当該送信側コンピュータ１に固有かつ秘密に保持された暗号鍵を用いてオリジナル文書を暗号化してネットワークを介して送信し、受信側コンピュータ２がこれを受信してプリンタ３に出力する。プリンタ３の制御部３２は、当該暗号化文書の入力を受けて、その暗号化文書を生成した送信側コンピュータ１に関連づけられている復号鍵を公開鍵サーバ４から取得し、当該復号鍵を用いて暗号化文書を復号処理し、復号の結果得られたオリジナル文書を印刷処理する。

【００３８】これにより、文書の提供元が正当であることを認証することができる。また、ここでは送信側コンピュータ１に暗号鍵が設定されている場合について説明したが、スキャナ等の入力装置に暗号鍵を設定し、このスキャナが、画像データを取り込むとともに、当該取り込んだ画像データを当該暗号鍵で暗号化処理して送信側コンピュータ１に出力するようにしてもよい。また、こ

の場合に、スキャナに磁気カードリーダを接続し、磁気カードに各利用者ごとの暗号鍵を記録して各利用者に配布しておくことで、利用者が磁気カードリーダに自己の磁気カードを読み取らせて、その暗号鍵をスキャナに読み取らせ、スキャナが磁気カードリーダから読み取った当該暗号鍵を用いて画像データの暗号化を行うようにしてもよい。

【００３９】すなわち、本実施の形態においてはオリジナル文書に対し送信側に固有に設定された秘密暗号鍵によって暗号化した暗号化文書を送信し、出力側で送信側の秘密暗号鍵に対応する公開復号鍵を用いて受信した暗号化文書を復号することで正当な文書提供元から当該文書が提供されたことを確認するものである。

【００４０】［実施形態３］さらに、この第２の実施の形態に係る提供元の確認処理を第１の実施の形態に係る文書配信システムと組み合わせても構わない。すなわち、本発明の第３の実施の形態に係る文書配信システムは、図１に示した第１の実施の形態に係る文書配信システムと同様の構成をとるものであるが、各部の動作が異なる。

【００４１】本実施の形態においては、送信側コンピュータ１は、事前に設定された秘密暗号鍵（第１暗号鍵）を用いてオリジナル文書を暗号化するとともに、当該オリジナル文書を印刷するべきプリンタ３に関連する暗号鍵（第２暗号鍵）を公開鍵サーバ４から取得する。そして第１暗号鍵により暗号化された暗号化文書（以下、区別のため第１暗号化文書と呼ぶ）をさらに第２暗号鍵で暗号化処理してもう一つの暗号化文書（第２暗号化文書）を生成する。そして、送信側コンピュータ１は、この第２暗号化文書を送信する。ここで、第１の実施の形態と同様に、当該第２暗号化文書に対し、オリジナル文書に対する閲覧専用文書を付加して文書コンテナを生成し、これを送信することも好ましい。

【００４２】受信側コンピュータ２は、第２暗号化文書を含んだ文書コンテナ受信して、当該文書コンテナに含まれている閲覧専用文書を取り出してディスプレイに表示する。また、この受信側コンピュータ２は、利用者からの指示に応じて当該文書コンテナに含まれている第２暗号化文書をプリンタ３に出力する。

【００４３】プリンタ３のデータインタフェース３１は、受信側コンピュータ２から入力されるデータを制御部３２に出力する。制御部３２は、入力されたデータが第２暗号化文書であるときには、記憶部３３に格納されている復号処理のプログラムに従って、記憶部３３に記憶されている、固有の復号鍵（第２暗号鍵に対応する復号鍵（以下、第２復号鍵と呼ぶ））を読み出して、この第２復号鍵で第２暗号化文書を復号化して、第１暗号化文書を抽出する。さらに制御部３２は、送信側コンピュータ１に関連づけて公開鍵サーバ４に記憶されている復号鍵（第１暗号鍵に対応する復号鍵（第１復号鍵と呼ぶ））を取得して、この抽出した第１暗号化文書を第１復号鍵を用いて復号化する。この処理によってオリジナル文書が取り出され、制御部３２は、当該オリジナル文書を印刷処理部３４に印刷させる。

【００４４】本実施の形態によると、第１暗号鍵と第１復号鍵とのペアによりオリジナル文書の提供元が正当であることが確認され、第２暗号鍵と第２復号鍵とのペアにより出力点が特定されて、セキュリティがさらに向上する。

【００４５】上記第１～第３の実施の形態の文書配信システムによると、入出力用のデバイスに秘密鍵が設定され、これを利用して入力元の認証、出力先の指定が可能となる。尚、ここではデバイスの例として、スキャナやプリンタ３に秘密鍵が設定されている場合について説明したが、これらに限らず、入力デバイスとしてのタブレットやキーボード、カメラに設定してもよいし、出力デバイスとしてのプロッタ、ディスプレイ装置等に設定されていてもよい。

【００４６】

【発明の効果】本発明によれば、文書の提供元に配置された文書提供装置が、オリジナル文書に基づき、所定の印刷装置でのみ復号可能な暗号化処理を行って得られた暗号化文書並びに、閲覧専用文書を生成し、当該生成した暗号化文書並びに、閲覧専用文書を文書コンテナとして配信し、文書取得装置が、文書提供装置から配信された文書コンテナを受信し、当該文書コンテナに含まれる閲覧専用文書を閲覧に供するとともに、指示に応じて当該文書コンテナに含まれる暗号化文書を、それを復号可能な印刷装置に出力し、印刷装置が、文書取得装置から入力される暗号化文書を復号化してオリジナル文書を再生する文書配信システムとしているので、当該再生したオリジナル文書の印刷を行って、文書提供装置側で選択した暗号化処理により、印刷先の印刷装置を提供元で特定可能となり、文書の出所を明確にしてセキュリティの向上を図ることができる。

【図面の簡単な説明】

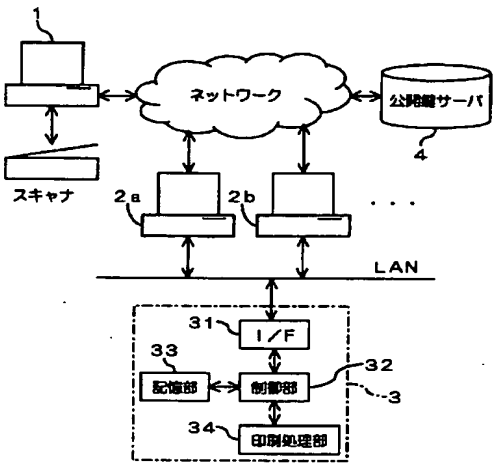
【図１】　本発明の実施の形態に係る文書配信システムの構成ブロック図である。

【図２】　公開鍵サーバの内容の一例を表す説明図である。

【符号の説明】

１　送信側コンピュータ、２　受信側コンピュータ、３　プリンタ、４　公開鍵サーバ、３１　データインタフェース、３２　制御部、３３　記憶部、３４印刷処理部。

【図１】



【図２】

プリンタ識別情報	暗号化鍵
aaaa	pppp・・・
bbbb	qqqq・・・
・	・
・	・
・	・